FortiAnalyzer - XML API Reference

VERSION 5.2.4

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

September 23, 2015

FortiAnalyzer 5.2.4 XML API Reference

05-524-293618-20150923

TABLE OF CONTENTS

Change Log

Date	Change Description
2015-09-04	Updated for version 5.2.3
2015-09-23	Updated for version 5.2.4

Introduction

FortiAnalyzer 5.2 includes a web services interface that facilitates integration with provision systems.

This guide describes how to use the XML-based FortiAnalyzer Application Programming Interface (API) to obtain information from the FortiAnalyzer unit, run scripts to modify device configurations, and install modified configurations to managed devices.

What's New in FortiAnalyzer 5.2.0

Element changes in FortiAnalyzer 5.2 Patch Release 1

The following element changes have been made in FortiAnalyzer 5.2 Patch Release 1:

- runFazReport
- Add filters to generate per user reports.

New elements in FortiAnalyzer 5.2 Patch Release 2

The following elements have been added in FortiAnalyzer 5.2 Patch Release 2:

- addPolicyPackage
- assignGlobalPolicy

New elements in FortiAnalyzer 5.2 Patch Release 3

No new elements were added in FortiAnalyzer 5.2 Patch Release 3.

Using the FortiAnalyzer API

The FortiAnalyzer enables you to configure managed FortiGate devices through a web services interface.

This sections includes the following topics:

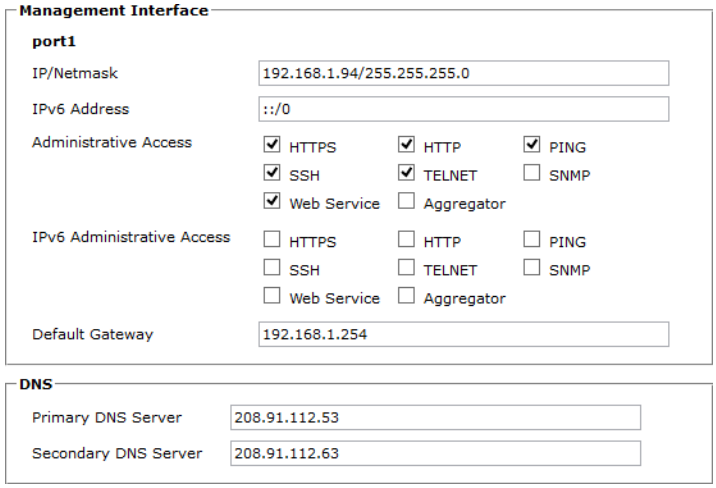
Connecting to FortiAnalyzer web services

Enabling web services

Web services must be enabled on the network interface that the client will connect to.

To enable web services on an interface with the GUI:

1. Go to *System Settings* > *Network* > *Interface*.
2. Select the *Edit* icon for the interface that you need to enable web services on.



3. In the *Administrative Access* section, select *Web Service*.
4. Select *OK* to apply the changes.

To enable web services on an interface using the CLI:

Enter the following command line interface (CLI) commands:

```
config system interface
     edit <port>
        set allowaccess webservice
     end
  end
```

where `<port>` is the network interface that you want to use for web services.

The `allowaccess` command should also include the other types of administrative access that you want to permit. For example, to allow HTTPS, SSH, and Web Services, enter the CLI command `set allowaccess https ssh webservice`.

The FortiAnalyzer unit handles web services requests on port 8080.

Obtaining the WSDL file

You can download the WDSL file from the GUI, or directly from your FortiAnalyzer at the following URL: https://<FortiAnalyzer_ip_address>:8080/

To download the WSDL file using the GUI:

1. Go to *System Settings* > *Advanced* > *Advanced Settings*
2. Select the *Download WSDL file* icon.
3. Save the `xml.wsdl` file to your local hard disk drive. You can open this file using a text editor.

By using a web testing tool, such as SoapUI, you can get information from your FortiAnalyzer.

Getting information from the FortiAnalyzer unit

To work with your managed devices, you need to obtain information from your FortiAnalyzer unit, such as:

- a list of ADOMs
- information about the managed devices
- information about individual devices
- the current configuration of devices, according to the database
- the revision history of devices.

SOAP error codes and descriptions

- SOAP_ERROR_OK = 0, /* same with SOAP_OK */
- SOAP_ERROR_DEFAUT_ZONE = -100, /* This is obsoleted */
- SOAP_ERROR_INVALID_PARAM = -101, /* invalid parameter(s) */
- SOAP_ERROR_PREPARE_PROBLEM = -102, /* prepare problem(s) */
- SOAP_ERROR_NOT_SUPPORTED = -103, /* not supported */
- SOAP_ERROR_FUNC_PROBLEM = -104, /* function problem */
- SOAP_ERROR_WRONG_CONDITION = -105, /* wrong condition(s) */
- SOAP_ERROR_MEMORY_LIMIT = -106, /* not enough memory */

Besides the *errorMsg* response, there could be errors returned in <SOAP-ENV:Fault> envelope as well. These are considered generic SOAP errors. There are also cases in which errors from the FortiAnalyzer application level are returned inside <SOAP-ENV:Fault> envelope. These errors are free-style; there are no error codes associated with them.

For example:

```
<SOAP-ENV:Fault>
   <faultcode>SOAP-ENV:Client</faultcode>
   <faultstring>Invalid admin uesr name '(null)'</faultstring>
   <detail>
   <error xmlns="http://localhost/">Invalid admin user name '(null)'</error>
   </detail>
</SOAP-ENV:Fault>
```

FortiAnalyzer XML API elements

addAdom

Use this request to add an ADOM to your FortiManager unit.

Example request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:addAdom>
         <!--Optional:-->
         <servicePass>
            <!--Optional:-->
            <userID>?</userID>
            <!--Optional:-->
            <password>?</password>
         </servicePass>
         <name>?</name>
         <version>?</version>
         <mr>?</mr>
         <!--Optional:-->
         <isBackupMode>?</isBackupMode>
         <!--Optional:-->
         <VPNManagement>?</VPNManagement>
         <!--Zero or more repetitions:-->
         <deviceSNVdom>
            <!--Optional:-->
            <SN>?</SN>
            <!--Zero or more repetitions:-->
            <vdomName>?</vdomName>
            <!--Zero or more repetitions:-->
            <vdomID>?</vdomID>
         </deviceSNVdom>
         <!--Zero or more repetitions:-->
         <deviceIDVdom>
            <!--Optional:-->
            <ID>?</ID>
            <!--Zero or more repetitions:-->
            <vdomName>?</vdomName>
            <!--Zero or more repetitions:-->
            <vdomID>?</vdomID>
         </deviceIDVdom>
   </r20:addAdom>
</soapenv:Body>.
```

Request Field	Description
<userID>	The administrator user name.

Request Field	Description
<password>	Administrator password options: Enter the administrator password or leave field blank for no password.
<name>	The name of the ADOM to be created.
<version>	Firmware version options: • `400`: FortiOS version 4.0. • `500`: FortiOS version 5.0.
<mr>	The firmware major release version.
<isBackupMode>	Backup Mode ADOM options: • true: `BackupMode` is enabled. • false: `BackupMode` is disabled.
<VPNManagement>	VPN console ADOM options: • true: VPN console is enabled. • false: VPN console is disabled.
<deviceSNVdom>	XML structure consists of serial number, VDOM name, and VDOM ID variables.
<SN>	Serial number of device.
<vdomName>	The name of the VDOM.
<vdomID>	The VDOM identifier.
<deviceIDVdom>	XML structure consists of device ID, VDOM name, and `VDOM identifier` variables.
<ID>	The VDOM ID.
<vdomName>	The name of the VDOM.
<vdomID>	The VDOM identifier.

The response indicates if the request was successful or if it failed.

Example response:

```
<SOAP-ENV:Header/>
<SOAP-ENV:Body>
   <ns3:addAdomResponse>
         <errorMsg>
            <errorCode>0</errorCode>
            <errorMsg>Add members to adom test successfully</errorMsg>
         </errorMsg>
   </ns3:addAdomResponse>
</SOAP-ENV:Body>
```

Response Field	Description
<errorMsg>	Indicates if the request was successful or if it failed. The error message consists of the error code and details.
<errorCode>	Error code and message details: • 0: Added members to the ADOM successfully. • -101: The user does not have permission to run this command. Cannot get ADOM OID. • -102: The global workspace is locked. Cannot get ADOM detail information. • -104: Cannot get ADOM detail information. • -106: Not enough memory.
<errorMsg>	

addDevice

Use this request to add a device to your FortiManager unit.

Example request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:addDevice>
      <!--Optional:-->
         <servicePass>
         <!--Optional:-->
         <userID>admin</userID>
         <!--Optional:-->
         <password></password>
      </servicePass>
      <!--Optional:-->
      <adom>root</adom>
      <!--Optional:-->
      <ip>1.1.1.1</ip>
      <!--Optional:-->
      <autod>manual</autod>
      <!--Optional:-->
      <deviceType>FortiGate</deviceType>
      <!--Optional:-->
      <name>test</name>
      <!--Optional:-->
      <adminUser>admin</adminUser>
      <!--Optional:-->
      <password></password>
      <!--Optional:-->
      <version>500</version>
      <!--Optional:-->
      <mr>0</mr>
      <!--Optional:-->
      <model>FortiGate-VM</model>
      <!--Optional:-->
      <flags></flags>
```

```
        <!--Optional:-->
        <description>sss</description>
        <!--Optional:-->
        <devId></devId>
        <!--Optional:-->
        <SN>FGVM001</SN>
        <!--Optional:-->
        <SNprefix>FGVM00</SNprefix>
      </r20:addDevice>
   </soapenv:Body>
```

Request Field	Description
<servicepass>	XML structure consists of username and password variables.
<userID>	The administrator user name.
<password>	Administrator password options: Enter the administrator password or leave field blank for no password.
<adom>	If the ADOM field is blank, the default ADOM will be that of the administrative user. If this administrator binds to all ADOMs, then the ADOM is root.
<ip>	The device IP address.
<autod>	autod options: `true`, `false`, `manual`, or `unreg` Select if you want to enable auto discovery. The default value is `False`. Select the value `unreg` to promote an unregistered device.
<deviceType>	Select the type of device. The device type can be: FortiGate, FortiCarrier, or FortiSwitch.
<name>	The host name of the device.
<adminUser>	The administrator user name.
<password>	Administrator password options: Enter the administrator password or leave field blank for no password.
<version>	Firmware version options: • `400`: FortiOS version 4.0. • `500`: FortiOS version 5.0.
<mr>	The firmware major release version.
<model>	The device model number, FGT-60C, for example.

Request Field	Description
<flags>	Flags options: • harddisk: The device has a hard disk installed. • No value: Leave this field blank if the device does not have a hard disk installed.
<description>	The device description (optional).
<devId>	The device identifier.
<SN>	The device serial number.
<SNprefix>	The device serial number prefix.

The response is a series of <return> tags, each containing information about the device.

Example response:

```
<SOAP-ENV:Header/>
<SOAP-ENV:Body>
   <ns3:addDeviceResponse>
         <errorMsg>
            <errorCode>0</errorCode>
            <errorMsg>Read task ID 10 to get addDevice result</errorMsg>
         </errorMsg>
         <taskId>10</taskId>
   </ns3:addDeviceResponse>
</SOAP-ENV:Body>
```

Response Field	Description
<errormsg>	Indicates if the request was successful or if it failed. The error message consists of the error code and detail.

Response Field	Description
<errorCode>	Error code and message details: • 0: Read task ID to get add device result. • -101: The device IP cannot be empty. The device name must be input. Administrator user must be input. Unknown device type; only accepts `FortiGate`, `FortiCarrier`, or `FortiSwitch`. The device firmware version (400, or 500) must be input. The device version should be 400 or 500 value is invalid. The device version mr (0, 1, etc...) must be input. The device version major release is invalid. The device model (FortiGate-200B, FortiWiFi-60C, etc...) must be input. The device model is invalid. The device ID must be set when promoting an unregistered device. Promotable device does not exist. The device is not an unregistered device. • -102: The ADOM is locked. • -103: Add device auto discovery mode is not supported yet. • -104: Add device by IP in ADOM failed. Promote device by device ID in ADOM failed.
<errorMsg>	
<taskid>	Indicates the task ID number.

deleteAdom

Use this request to delete an ADOM from your FortiManager unit.

Example request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:deleteAdom>
         <servicePass>
            <userID>?</userID>
            <password>?</password>
         </servicePass>
            <adomName>?</adomName>
            <adomOid>?</adomOid>
   </r20:deleteAdom>
</soapenv:Body>
```

Request Field	Description
<servicepass>	XML structure consists of username and password variables.
<userID>	The administrator user name.
<password>	Administrator password options: Enter the administrator password or leave field blank for no password.

Request Field	Description
<adomName>	The name of the ADOM.
<adomOid>	The ADOM object identifier (OID).

The response indicates with the request was successful or if it failed.

Example response:

```
<SOAP-ENV:Header/>
<SOAP-ENV:Body>
   <ns3:deleteAdomResponse>
         <errorMsg>
            <errorCode>0</errorCode>
            <errorMsg>Delete adom ID 166 successfully</errorMsg>
         </errorMsg>
   </ns3:deleteAdomResponse>
</SOAP-ENV:Body>
```

Response Field	Description
<errorMsg>	Indicates if the request was successful or if it failed. The error message consists of the error code and detail.
<errorCode>	Error code and message details: • 0: Deleted ADOM ID successfully. • -101: The ADOM name is invalid. Cannot get a valid ADOM ID. Invalid ADOM. • -102: The ADOM is locked. The global workspace is locked. • -104: The ADOM ID cannot be deleted. • -105: The root ADOM cannot be deleted. The ADOM ID is in use and cannot be deleted.
<errorMsg>	

deleteDevice

Use this request to delete a device defined on your FortiManager unit.

Example request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:deleteDevice>
         <servicePass>
            <password></password>
            <userID>admin</userID>
         </servicePass>
            <devId>468985</devId>
            <serialNumber>FGT60C3G06500185</serialNumber>
   </r20:deleteDevice>
</soapenv:Body>
```

Request Field	Description
<servicePass>	XML structure consists of username and password variables.
<userID>	The administrator user name.
<password>	Administrator password options: Enter the administrator password or leave field blank for no password.
<devId>	The device ID number.
<serialNumber>	The serial number of device.

The response indicates if the device was deleted successfully or if the procedure failed.

Example response:

```
<SOAP-ENV:Header/>
<SOAP-ENV:Body>
   <ns3:deleteDeviceResponse>
         <errorMsg>
            <errorCode>0</errorCode>
            <errorMsg>Delete device ID 468985 successfully</errorMsg>
         </errorMsg>
   </ns3:deleteDeviceResponse>
</SOAP-ENV:Body>
```

Response Field	Description
<errorMsg>	Indicates if the request was successful or if it failed. The error message consists of the error code and detail.
<errorCode>	Error code and message details: • 0: Read task ID to get delete device result. • -102: The ADOM is locked. • -104: The device can only be deleted from the ADOM which contains its root VDOM. The device ID cannot be deleted. • -105: The device ID is in use and cannot be deleted. The device ID was locked and cannot be deleted.
<errorMsg>	

editAdom

Use this request to edit an ADOM.

Example request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:editAdom>
         <!--Optional:-->
         <servicePass>
```

```
            <!--Optional:-->
            <userID>?</userID>
            <!--Optional:-->
            <password>?</password>
         </servicePass>
         <name>?</name>
         <!--Optional:-->
         <version>?</version>
         <!--Optional:-->
         <mr>?</mr>
         <!--Optional:-->
         <state>?</state>
         <!--Optional:-->
         <isBackupMode>?</isBackupMode>
         <!--Optional:-->
         <VPNManagement>?</VPNManagement>
         <!--Optional:-->
         <metafields>
            <!--Zero or more repetitions:-->
            <metafield>
               <name>?</name>
               <value>?</value>
            </metafield>
         </metafields>
         <!--Zero or more repetitions:-->
         <addDeviceSNVdom>
            <!--Optional:-->
            <SN>?</SN>
            <!--Zero or more repetitions:-->
            <vdomName>?</vdomName>
            <!--Zero or more repetitions:-->
            <vdomID>?</vdomID>
            </addDeviceSNVdom>
         <!--Zero or more repetitions:-->
         <addDeviceIDVdom>
            <!--Optional:-->
            <ID>?</ID>
            <!--Zero or more repetitions:-->
            <vdomName>?</vdomName>
            <!--Zero or more repetitions:-->
            <vdomID>?</vdomID>
         </addDeviceIDVdom>
      </r20:editAdom>
   </soapenv:Body>
```

Request Field	Description
<servicePass>	XML structure consists of username and password variables.
<userID>	The administrator user name.
<password>	Administrator password options: • Enter the administrator password • Leave field blank for no password

Request Field	Description
<name>	The name of the ADOM to be edited.
<version>	Firmware version options: • 400: FortiOS version 4.0. • 500: FortiOS version 5.0.
<mr>	The firmware major release version.
<state>	Device ADOM state options: • true: ADOMs are enabled • false: ADOMs are disabled
<isBackupMode>	Backup Mode ADOM options: • true: BackupMode is enabled. • false: BackupMode is disabled.
<VPNManagement>	VPN console ADOM options: • true: VPN console is enabled. • false: VPN console is disabled.
<metafields>	XML structure consists of metafield data. These strings occur in pairs in XML responses.
<name>	Name of device metafield (s).
<value>	Value of device metafield (s).
<addDeviceSNVdom>	XML structure consists of serial number, VDOM name, and VDOM ID variables.
<SN>	Serial number of device, FGT60C3G06500185, for example.
<vdomName>	The name of the VDOM.
<vdomID>	The VDOM identifier.
<addDeviceIDVdom>	XML structure consists of the device ID, VDOM name, and VDOM ID variables.
<ID>	The ID of the device.
<vdomName>	The name of the VDOM.
<vdomID>	The VDOM identifier.

The response indicates if the request was successful or if it failed.

Example response:

```
<SOAP-ENV:Header/>
<SOAP-ENV:Body>
   <ns3:editAdomResponse>
         <errorMsg>
         <errorCode>0</errorCode>
            <errorMsg>Edit adom root successfully</errorMsg>
         </errorMsg>
   </ns3:editAdomResponse>
</SOAP-ENV:Body>
```

<table>
<tr><th>Response Field</th><th>Description</th></tr>
<tr><td><errorMsg></td><td>Indicates if the request was successful or if it failed. The error message consists of the error code and detail.</td></tr>
<tr><td><errorCode></td><td rowspan="2">Error code and message details:
• 0: Edited ADOM name successfully.
• -101: The ADOM name cannot be empty. The ADOM name is invalid. Version only accepts 400 or 500 values. Invalid major release value. The ADOM metafield does not exist. The metafield name does not exist. Failed to change ADOM information.
• -102: The global workspace is locked. Failed to get ADOM information. Failed to get ADOM flags. Failed to create device fetch. Cannot change mode to backup mode since the ADOM has device(s). Cannot get ADOM metafields.
• -104: Adding members to ADOM failed.</td></tr>
<tr><td><errorMsg></td></tr>
</table>

getAdomList

Use this request to get a list of the ADOMs defined on your FortiManager unit. Only an administrator with the `Super_User` profile can run this command.

Example request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:getAdomList>
         <!--Optional:-->
         <servicePass>
            <!--Optional:-->
            <userID>?</userID>
            <!--Optional:-->
            <password>?</password>
         </servicePass>
         <!--Optional:-->
         <detail>?</detail>
   </r20:getAdomList>
</soapenv:Body>
```

Request Field	Description
<servicePass	XML structure consists of username and password variables.
<userID>	The administrator user name.
<password>	Administrator password options: • Enter the administrator password • Leave field blank for no password
<detail>	Detail field options: true or false

The response is a series of <return> tags, each containing information about an ADOM.

Example response: detail is true

```
<SOAP-ENV:Header/>
<SOAP-ENV:Body>
   <ns3:getAdomListResponse>
         <errorMsg>
            <errorCode>0</errorCode>
            <errorMsg>get adom detail list successfully</errorMsg>
         </errorMsg>
         <adomDetail>
            <oid>103</oid>
            <name>others</name>
            <description/>
            <version>500</version>
            <mr>0</mr>
            <state>true</state>
            <isBackupMode>false</isBackupMode>
            <VPNManagement>true</VPNManagement>
            <metafields>
               <metafield>
                  <name>meta1</name>
                  <value/>
               </metafield>
            </metafields>
         </adomDetail>
         <adomDetail>
            <oid>3</oid>
            <name>root</name>
            <description/>
            <version>500</version>
            <mr>0</mr>
            <state>true</state>
            <isBackupMode>false</isBackupMode>
            <VPNManagement>true</VPNManagement>
            <metafields>
            <metafield>
               <name>meta1</name>
               <value/>
            </metafield>
         </metafields>
         </adomDetail>
```

```
            <adomDetail>
               <oid>160</oid>
               <name>test1</name>
               <description/>
               <version>500</version>
               <mr>1</mr>
               <state>true</state>
               <isBackupMode>false</isBackupMode>
               <VPNManagement>false</VPNManagement>
               <metafields>
                  <metafield>
                     <name>meta1</name>
                     <value>me</value>
                  </metafield>
            </metafields>
            </adomDetail>
      </ns3:getAdomListResponse>
   </SOAP-ENV:Body>
```

Example response: (detail is false)

```
   <SOAP-ENV:Header/>
   <SOAP-ENV:Body>
      <ns3:getAdomListResponse>
            <errorMsg>
               <errorCode>0</errorCode>
               <errorMsg>get adom list successfully</errorMsg>
            </errorMsg>
            <adomInfo>
               <oid>103</oid>
               <name>others</name>
               <description/>
               <version>500</version>
               <mr>0</mr>
               <state>true</state>
            </adomInfo>
            <adomInfo>
               <oid>3</oid>
               <name>root</name>
               <description/>
               <version>500</version>
               <mr>0</mr>
               <state>true</state>
            </adomInfo>
            <adomInfo>
               <oid>160</oid>
               <name>test1</name>
               <description/>
               <version>500</version>
               <mr>1</mr>
               <state>true</state>
            </adomInfo>
      </ns3:getAdomListResponse>
   </SOAP-ENV:Body>
```

Response Field	Description
<errorMsg>	Indicates if the request was successful or if it failed. The error message consists of the error code and detail.
<errorCode>	Error code and message details: • 0: Retrieved ADOM list successfully. Retrieved ADOM detail list successfully. • -104: ADOM fetch error. Cannot get ADOM basic information. Cannot get ADOM detail information. • -106: Not enough memory.
<errorMsg>	
<adomDetail>	XML structure consists of the object identifier, ADOM name, and description.
<oid>	The object identifier.
<name>	The ADOM name.
<description>	A description of the ADOM.
<version>	Firmware version options: • `400`: FortiOS version 4.0. • `500`: FortiOS version 5.0.
<mr>	The firmware major release version.
<state>	Device ADOM state options: • true: ADOMs are enabled. • false: ADOMs are disabled.
<isBackupMode>	Backup Mode ADOM options: • true: `BackupMode` is enabled. • false: `BackupMode` is disabled.
<VPNManagement>	VPN console ADOM options: • true: VPN console is enabled. • false: VPN console is disabled.
<metafield>	XML structure consists of metafield data. These strings occur in pairs in XML responses.
<name>	Name of device metafield (s).
<value>	Value of device metafield (s).

getAdoms

Use this request to get a list of ADOMs.

Example request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:getAdoms>
         <!--Optional:-->
         <servicePass>
            <!--Optional:-->
            <userID>?</userID>
            <!--Optional:-->
            <password>?</password>
         </servicePass>
         <!--Zero or more repetitions:-->
         <names>?</names>
         <!--Zero or more repetitions:-->
         <adomIds>?</adomIds>
   </r20:getAdoms>
</soapenv:Body>
```

Request Field	Description
<servicePass>	XML structure consists of username and password variables.
<userID>	The administrator user name.
<password>	Administrator password options: • Enter the administrator password. • Leave field blank for no password.
<names>	The ADOM name.
<adomIDs>	The ADOM object ID.

The response indicates if the request was successful or if it failed.

Example response:

```
<SOAP-ENV:Header/>
<SOAP-ENV:Body>
   <ns3:getAdomsResponse>
         <errorMsg>
            <errorCode>0</errorCode>
            <errorMsg>Get adoms info Successfully</errorMsg>
         </errorMsg>
         <adomDetail>
            <oid>3</oid>
            <name>root</name>
            <description/>
            <version>5</version>
```

```
            <mr>0</mr>
            <state>true</state>
            <isBackupMode>false</isBackupMode>
            <VPNManagement>true</VPNManagement>
          <metafields>
            <metafield>
              <name>meta1</name>
              <value/>
            </metafield>
          </metafields>
          </adomDetail>
    </ns3:getAdomsResponse>
  </SOAP-ENV:Body>
```

Response Field	Description
<errorMsg>	Indicates if the request was successful or if it failed. The error message consists of the error code and detail.
<errorCode> <errorMsg>	Error code and message details: • 0: Retrieved ADOM information successfully. • -101: Invalid admin user name. User does not have permission to run this command. Cannot get ADOM OID. • -102: Cannot get ADOM detail information. • -104: Cannot get ADOM detail information. • -106: Not enough memory.
<adomDetail>	XML structure consists of the object identifier, ADOM name, description, firmware version, and major release.
<oid>	The object identifier for the ADOM.
<name>	The name of the ADOM.
<description>	A description of the ADOM.
<version>	Firmware version options: • `400`: FortiOS version 4.0. • `500`: FortiOS version 5.0.
<mr>	The firmware major release version.
<state>	Device ADOM state options: • true: ADOMs are enabled. • false: ADOMs are disabled.
<isBackupMode>	Backup Mode ADOM options: • true: `BackupMode` is enabled. • false: `BackupMode` is disabled.

Response Field	Description
<VPNManagement>	VPN console ADOM options: • true: VPN console is enabled. • false: VPN console is disabled.
<metafield>	XML structure consists of metafield data. These strings occur in pairs in XML responses.
<name>	Name of device metafield (s).
<value>	Value of device metafield (s).

getDeviceList

Use this request to get summary information about the managed devices, optionally limited to a particular ADOM.

Example request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:getDeviceList>
         <!--Optional:-->
         <servicePass>
            <!--Optional:-->
            <userID>?</userID>
            <!--Optional:-->
            <password>?</password>
         </servicePass>
         <!--Optional:-->
         <adom>?</adom>
         <!--Optional:-->
         <detail>?</detail>
   </r20:getDeviceList>
</soapenv:Body>
```

Request Field	Description
<servicePass>	XML structure consists of username and password variables.
<userID>	The administrator user name.
<password>	Administrator password options: • Enter the administrator password. • Leave field blank for no password.

Request Field	Description
<adom>	If the ADOM field is blank, the default ADOM will be that of the administrative user. If this administrator binds to all ADOMs, then the ADOM is root.
<detail>	Detail field options: true, or false

The response is a series of <return> tags, each containing information about a device.

Example response: (detail is true)

```
<SOAP-ENV:Header/>
<SOAP-ENV:Body>
   <ns3:getDeviceListResponse>
         <errorMsg>
            <errorCode>0</errorCode>
            <errorMsg>get device detail list successfully</errorMsg>
         </errorMsg>
         <deviceDetail>
            <devId>129</devId>
            <firmware>FortiGate</firmware>
            <firmwareVersion>5</firmwareVersion>
            <buildNum>128</buildNum>
            <description/>
            <hostname>FGT60C3G06500185</hostname>
            <platform>FortiGate-60C</platform>
            <sn>FGT60C3G06500185</sn>
            <ip>10.2.60.99</ip>
            <IPSContract>3.00249(2012-10-11 02:47)</IPSContract>
            <antiVirusContract>16.00560(2012-10-19 08:31)</antiVirusContract>
            <appsignature/>
            <mgmtMode>reg</mgmtMode>
         </deviceDetail>
   </ns3:getDeviceListResponse>
</SOAP-ENV:Body>
```

Example response: (detail is false)

```
<SOAP-ENV:Header/>
<SOAP-ENV:Body>
   <ns3:getDeviceListResponse>
         <errorMsg>
            <errorCode>0</errorCode>
            <errorMsg>get device list successfully</errorMsg>
         </errorMsg>
         <deviceInfo>
            <devId>129</devId>
            <firmware>FortiGate</firmware>
            <firmwareVersion>5</firmwareVersion>
            <buildNum>128</buildNum>
            <description/>
            <hostname>FGT60C3G06500185</hostname>
            <platform>FortiGate-60C</platform>
            <sn>FGT60C3G06500185</sn>
```

```
            <ip>10.2.60.99</ip>
          </deviceInfo>
      </ns3:getDeviceListResponse>
  </SOAP-ENV:Body>
```

Response Field	Description
<errorMsg>	Indicates if the request was successful or if it failed. The error message consists of the error code and detail.
<errorCode>	Error code and message details: • 0: Retrieved device list successfully. Retrieved device detail list successfully. • -102: Device fetch error for ADOM. • -104: Cannot get device detail information.
<errorMsg>	
<deviceDetail>	XML structure consists of the following tags.
<devID>	The Device ID. This is the primary device identifier.
<firmware>	FortiGate, FortiCarrier, or FortiSwitch
<firmwareVersion>	Version of device operating system, 5, for example for FortiOS 5.0.
<buildNum>	Firmware version build number, 0128, for example.
<description>	Device description from FortiManager database.
<hostname>	The device host name.
<platform>	Platform name for device, FortiGate-60C, for example.
<sn>	Serial number of device, FGT60C3G06500185, for example.
<ip>	IP address of device network interface from which response was received.
<IPSContract>	FortiGuard IPS definitions version and last update time, 2.00461(2008-12-08 11:23), for example.
<antiVirusContract>	AV contract and expiry date, 8.00631(2012-02-15 14:27), for example.
<appsignature>	FortiGuard application signature.
<mgmtMode>	The device management mode. One of the following: • reg: Registered device • unreg: Unregistered device • unknown: Device registration status is unknown.

getDevices

Use this request to get information about specific managed devices, identified by serial number or device ID. You can obtain device ID values by using the `execute dmserver showdev` CLI command.

If you want information about the device's configuration, see getFazConfig on page 34.

Example request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:getDevices>
         <servicePass>
            <password></password>
            <userID>admin</userID>
         </servicePass>
         <serialNumbers>FGT60C3G06500185</serialNumbers>
         <serialNumbers>FGT60C3G06500186</serialNumbers>
   </r20:getDevices>
</soapenv:Body>
```

Request Field	Description
<servicePass>	XML structure consists of username and password variables.
<userID>	The administrator user name.
<password>	Administrator password options: • Enter the administrator password. • Leave field blank for no password.
<serialNumbers>	Serial number of the device. This is the secondary identifier. You can enter multiple serial numbers fields.
<devIds>	Device ID. This is the primary device identifier. You can omit this field and use the serial number instead. You can enter multiple device ID fields.

The response is a series of <return> tags, each containing information about a device.

Example response:

```
<SOAP-ENV:Header/>
<SOAP-ENV:Body>
   <ns3:getDevicesResponse>
         <return>
            <firmware>FortiGate</firmware>
            <firmwareVersion>5</firmwareVersion>
            <buildNum>128</buildNum>
            <description/>
            <hostname>Dev3</hostname>
            <IPSContract>2.442(2012-11-08 11:23)</IPSContract>
            <antiVirusContract>8.368(2007-11-15 13:59)</antiVirusContract>
            <platform>FortiGate-60C</platform>
```

```
            <sn>FGT60C3G06500185</sn>
            <ip>172.20.120.126</ip>
         </return>
         <return>
            <firmware>FortiGate</firmware>
            <firmwareVersion>5</firmwareVersion>
            <buildNum>128</buildNum>
            <description/>
            <hostname>FGT60C3G06500185</hostname>
            <IPSContract/>
            <antiVirusContract/>
            <platform>Fortigate-60C</platform>
            <sn>FGT60C3G06500186</sn>
            <ip>172.20.120.127</ip>
         </return>
      </ns3:getDevicesResponse>
   </SOAP-ENV:Body>
```

Response Field	Description
<errorMsg>	Indicates if the request was successful or if it failed. The error message consists of the error code and detail.
<errorCode>	Error code and message details: • 0: Retrieved device(s) information successfully. • -102: Serial number is not found. Cannot get device information. • -104: Cannot get device information.
<errorMsg>	
<firmware>	One of: • FortiGate • FortiCarrier • FortiSwitch
<firmwareVersion>	Version of device operating system, 500, for example for FortiOS 5.0.
<buildNum>	Firmware version build number, 0128, for example.
<description>	Device description from database.
<hostname>	The device host name.
<IPSContract>	FortiGuard IPS definitions version and last update time, 2.00461(2012-11-08 11:23), for example.
<antiVirusContract>	AV contract and expiry date, 8.00631(2012-02-15 14:27), for example.
<platform>	Platform name for device, FortiGate-60C, for example.
<sn>	Serial number of device, FGT60C3G06500185, for example.
<ip>	IP address of device network interface from which response was received.

getDeviceVdomList

Use this request to obtain a list of device VDOMs.

Example request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:getDeviceVdomList>
         <!--Optional:-->
         <servicePass>
            <!--Optional:-->
            <userID>?</userID>
            <!--Optional:-->
            <password>?</password>
         </servicePass>
         <!--Optional:-->
         <devName>?</devName>
         <!--Optional:-->
         <devID>?</devID>
   </r20:getDeviceVdomList>
</soapenv:Body>
```

Request Field	Description
<password>	Administrator password options: • Enter the administrator password. • Leave field blank for no password.
<user>	The administrator user name.
<devName>	Name of the device host.
<devId>	The Device ID. This is the primary device identifier.

The response indicates if the request was successful or if it failed.

Example response:

```
<SOAP-ENV:Header/>
<SOAP-ENV:Body>
   <ns3:getDeviceVdomListResponse>
         <errorMsg>
            <errorCode>0</errorCode>
            <errorMsg>Get device 114 vdom list successfully</errorMsg>
         </errorMsg>
         <name>FGT60C3G06500185</name>
         <oid>114</oid>
         <return>
            <name>root</name>
            <oid>3</oid>
         </return>
   </ns3:getDeviceVdomListResponse>
```

```
</SOAP-ENV:Body>
```

Response Field	Description
<errorMsg>	Indicates if the request was successful or if it failed. The error message consists of the error code and detail.
<errorCode>	Error code and message details: • 0: Retrieved device VDOM list successfully. • -101: Cannot find the device by provided name or ID.
<errorMsg>	
<name>	The name of the VDOM device list.
<oid>	The object identifier.

getFazArchive

Use this request to get a FortiAnalyzer archive file. You need to input the device ID, archive type and the archive file name.

Example request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:getFazArchive>
      <!--Optional:-->
      <servicePass>
         <!--Optional:-->
         <userID>admin</userID>
         <!--Optional:-->
         <password></password>
      </servicePass>
      <!--Optional:-->
      <adom>root</adom>
      <!--Optional:-->
      <devId>FG200B0000000001</devId>
      <type>IPS</type>
      <!--Optional:-->
      <fileName>50005:0</fileName>
      <zipPassword></zipPassword>>
   </r20:getFazArchive>
</soapenv:Body>
```

Request Field	Description
<servicePass>	XML structure consists of username and password variables.
<userID>	The administrator user name.
<password>	Administrator password options: Enter the administrator password or leave field blank for no password.

Request Field	Description
<adom>	The ADOMs for which you want to get archives from.
<devId>	The device ID you want to get archives from.
<type>	The archive type. Archive type options: • 0: Web • 1: Email • 2: FTP • 3: IM • 4: MMS • 5: Quarantine • 6: IPS
<fileName>	The archive file name. You can check the name under *Log View* > *Archive*.
<zipPassword>	The password set for the zip file.
<filelist>	The archive file list.
<filename>	The archive file name will be displayed under this element.
<data>	The archive file content data. The data is base64 encoded, you need to decode the data before use.

The response will contain the binary data if the archive file in a base64 encoded message.

Example response:

```
<SOAP-ENV:Header/>
<SOAP-ENV:Body>
   <ns3:getFazArchiveResponse>
      <errorMsg>
         <errorCode>0</errorCode>
         <errorMsg>getFazArchive successfully</errorMsg>
      </errorMsg>
      <fileList>
      <fileName>50005:0</fileName>
         <data>
         =</data>
         <error>None</error>
      </fileList>
   </ns3:getFazArchiveResponse>
</SOAP-ENV:Body>
```

Request Field	Description
<errorMsg>	Indicates if the request was successful or if it failed. The error message consists of the error code and detail.

Request Field	Description
<errorCode>	Error code and message details: • -101: Invalid username, password, or ADOM. Cannot get device ID. Cannot get file name. Cannot get type. Cannot get checksum. Cannot get content filename. • -104: Cannot get content archive. Get FortiAnalyzer archive failed, no such file name. Get FortiAnalyzer archive failed, error reading file name. • -106: Not enough memory.
<errorMsg>	
<filelist>	The archive file list.
<filename>	The archive file name will be displayed under this element.
<data>	The archive file content data. The data is base64 encoded, you need to decode the data before use.

getFazConfig

Use this request to get the FortiAnalyzer configuration.

Example request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:getFazConfig>
      <!--Optional:-->
      <servicePass>
         <!--Optional:-->
         <userID>admin</userID>
         <!--Optional:-->
         <password></password>
      </servicePass>
   </r20:getFazConfig>
</soapenv:Body>
```

Request Field	Description
<servicePass>	XML structure consists of username and password variables.
<userID>	The administrator user name.
<password>	Administrator password options: Enter the administrator password or leave field blank for no password.

The response indicates if the request was successful or if it failed.

Example response:

```
<SOAP-ENV:Header/>
```

```
<SOAP-ENV:Body>
   <ns3:getFazConfigResponse>
   <errorMsg>
   <errorCode>0</errorCode>
   <errorMsg>getFazConfig successfully</errorMsg>
   </errorMsg>
   <config>#config-version=FAZVM-5.0-FW-build115-130121
   config system global
      set adom-mode normal
      set hostname "FMG-VM"
   end
   config system interface
      edit "port1"
         set ip 172.16.106.254 255.255.255.0
         set allowaccess ping https ssh http webservice
         set serviceaccess fgtupdates webfilter-antispam webfilter antispam
            config ipv6
            end
      next
      edit "port2"
         set ip 1.2.2.2 255.255.255.0
         set allowaccess ping https ssh http webservice
         set serviceaccess fgtupdates webfilter-antispam webfilter antispam
            config ipv6
            end
      next
      edit "port3"
            config ipv6
            end
      next
      edit "port4"
            config ipv6
            end
      next
   end
   config system snmp sysinfo
   end
   config system route
      edit 1
         set device "port1"
         set gateway 172.16.106.1
      next
   end
   config system dns
      set primary 208.91.112.53
      set secondary 208.91.112.63
   end
   config system ha
   end
   config system ntp
   config ntpserver
      edit 1
         set server "ntp1.fortinet.net"
      next
      end
         set status enable
         set sync_interval 1
```

```
end
config system backup all-settings
end
config system metadata admins
   edit "Contact Email"
      set importance optional
   next
   edit "Contact Phone"
      set importance optional
   next
end
config system admin profile
   edit "Restricted_User"
      set description "Restricted user profiles have no System Privileges enabled, and
          have read-only access for all Device Privileges."
      set device-manager read
      set device-config read
      set device-profile read
      set policy-objects read
      set deploy-management read
      set config-retrieve read
      set term-access read
      set adom-policy-packages read
      set adom-policy-objects read
      set vpn-manager read
      set realtime-monitor read
      set forticonsole read
      set consistency-check read
      set faz-management read
      set log-viewer read
      set report-viewer read
   next
   edit "Standard_User"
      set description "Standard user profiles have no System Privileges enabled, but
          have read/write access for all Device Privileges."
      set adom-switch read-write
      set global-policy-packages read-write
      set global-objects read-write
      set device-manager read-write
      set device-config read-write
      set device-op read-write
      set device-profile read-write
      set policy-objects read-write
      set deploy-management read-write
      set config-retrieve read-write
      set term-access read-write
      set adom-policy-packages read-write
      set adom-policy-objects read-write
      set vpn-manager read-write
      set realtime-monitor read-write
      set forticonsole read-write
      set consistency-check read-write
      set faz-management read-write
      set log-viewer read-write
      set report-viewer read-write
   next
   edit "Super_User"
```

```
        set description "Super user profiles have all system and device privileges
            enabled."
        set system-setting read-write
        set adom-switch read-write
        set global-policy-packages read-write
        set global-objects read-write
        set assignment read-write
        set read-passwd read-write
        set device-manager read-write
        set device-config read-write
        set device-op read-write
        set device-profile read-write
        set policy-objects read-write
        set deploy-management read-write
        set config-retrieve read-write
        set term-access read-write
        set adom-policy-packages read-write
        set adom-policy-objects read-write
        set vpn-manager read-write
        set realtime-monitor read-write
        set forticonsole read-write
        set consistency-check read-write
        set faz-management read-write
        set log-viewer read-write
        set report-viewer read-write
    next
    edit "Package_User"
        set description "Package user profile have read/write policy package and objects
            privileges enabled, and have read-only access for system and others
            privileges."
        set system-setting read
        set adom-switch read
        set global-policy-packages read-write
        set global-objects read-write
        set assignment read
        set read-passwd read
        set device-manager read-write
        set device-config read-write
        set device-op read-write
        set device-profile read-write
        set policy-objects read-write
        set deploy-management read-write
        set config-retrieve read
        set term-access read
        set adom-policy-packages read-write
        set adom-policy-objects read-write
        set vpn-manager read-write
        set realtime-monitor read
        set forticonsole read
        set consistency-check read
        set faz-management read
        set log-viewer read
        set report-viewer read
    next
end
config system certificate ca
end
```

```
config system certificate local
end
config system password-policy
end
config system admin user
   edit "admin"
      set trusthost2 0.0.0.0 0.0.0.0
      set trusthost3 127.0.0.1 255.255.255.255
      set ipv6_trusthost2 ::/0
      set ipv6_trusthost3 ::1/128
      set profileid "Super_User"
      set adom "all_adoms"
      set policy-package "all_policy_packages"
config dashboard
   edit 1
      set name "System Information"
      set column 1
      set refresh-interval 0
      set tabid 1
      set widget-type sysinfo
      next
   edit 2
      set name "System Resources"
      set column 1
      set refresh-interval 0
      set tabid 1
      set widget-type sysres
      set res-view-type real-time
      next
   edit 3
      set name "License Information"
      set column 2
      set refresh-interval 0
      set tabid 1
      set widget-type licinfo
      next
   edit 4
      set name "Unit Operation"
      set column 2
      set refresh-interval 0
      set tabid 1
      set widget-type sysop
      next
   edit 5
      set name "Alert Message Console"
      set column 2
      set refresh-interval 0
      set tabid 1
      set widget-type alert
      set num-entries 0
      next
   end
   next
end
config system admin setting
end
config system alertemail
```

```
end
config system mail
   edit "mail.fortinet.com"
      set auth enable
      set passwd ENC
          26ITYiEXHPFvx8y3vZqI4PPt2dH0OXAWPB3sVNcK+2nPTGyeRN1FMB+hJIlyHsyzchBxBmA2EMZEj
          y4gR5vBnYiufPp2Q5rcGhSAYqGQ2zMSt79R
      set user "jsmith@fortinet.com"
      next
   end
config system alert-console
end
config system log fortianalyzer
end
config system locallog disk setting
end
config system locallog disk filter
end
config system locallog memory setting
end
config system locallog memory filter
end
config system locallog fortianalyzer setting
end
config system locallog fortianalyzer filter
end
config system locallog syslogd setting
end
config system locallog syslogd filter
end
config system locallog syslogd2 setting
end
config system locallog syslogd2 filter
end
config system locallog syslogd3 setting
end
config system locallog syslogd3 filter
end
config system fips
end
config fmupdate av-ips fgt server-override
end
config fmupdate av-ips fct server-override
end
config fmupdate web-spam fgt server-override
end
config fmupdate web-spam fct server-override
end
config fmupdate av-ips push-override
end
config fmupdate av-ips push-override-to-client
end
config fmupdate web-spam poll-frequency
end
config fmupdate av-ips web-proxy
end
config fmupdate web-spam web-proxy
```

```
    end
    config fmupdate fct-services
    end
    config fmupdate av-ips advanced-log
    end
    config fmupdate av-ips update-schedule
    end
    config fmupdate analyzer virusreport
    end
    config fmupdate service
    end
    config fmupdate publicnetwork
    end
    config fmupdate disk-quota
    end
    config fmupdate server-access-priorities
    end
    config fmupdate web-spam fgd-setting
    end
    config fmupdate web-spam fgd-log
    end
    config fmupdate custom-url-list
    end
    config fmupdate device-version
    end
    config fmupdate deployment
    end
    config fmupdate server-override-status
    end
    config fmupdate multilayer
    end
    config fmupdate support-pre-fgt43
    end
    config system dm
    end
    config system log settings
    config rolling-regular
    end
    end
       config system sql
          set start-time 09:37 2013/01/18
       end
    </config>
    </ns3:getFazConfigResponse>
  </SOAP-ENV:Body>
```

Request Field	Description
<errorMsg>	Indicates if the request was successful or if it failed. The error message consists of the error code and detail.

Request Field	Description
<errorCode>	Error code and message details: • -101: Invalid username or password. • -102: Cannot allocate temp file. Cannot create configuration file. Cannot open file. • -106: Not enough memory.
<errorMsg>	
<config>	The device configuration.

getFazGeneratedReports

Use this request to get a completed historical report. To use this command, you need to input the report name, report date, compression method in the request.

Example request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:getFazGeneratedReport>
      <!--Optional:-->
      <servicePass>
         <!--Optional:-->
         <userID>admin</userID>
         <!--Optional:-->
         <password></password>
      </servicePass>
      <!--Optional:-->
      <adom>root</adom>
      <!--Optional:-->
      <reportDate>2013_01_24</reportDate>
      <!--Optional:-->
      <reportName>S-4_t4-2013-01-24-1611</reportName>
      <!--Optional:-->
      <compression>tar</compression>
   </r20:getFazGeneratedReport>
</soapenv:Body>
```

Request Field	Description
<servicePass>	XML structure consists of username and password variables.
<userID>	The administrator user name.
<password>	Administrator password options: Enter the administrator password or leave field blank for no password.
<adom>	The ADOMs for which you want to get a report from.

Request Field	Description
<reportDate>	The report generation date; in the format YYYY_MM_DD.
<reportName>	The generated report name. For example, S-schedule-utm-reports_t1-2013-01-24-1022.
<compression>	The compression type of the report that will be returned by this command. Compression options include: • 0: tar • 1: gzip

The report data returned in the response message is base64 encoded binary data. You need to decode it and then decompress it to get the report files.

Example response:

```
<SOAP-ENV:Header/>
<SOAP-ENV:Body>
   <ns3:getFazGeneratedReportResponse>
      <errorMsg>
         <errorCode>0</errorCode>
         <errorMsg>getFazGeneratedReport successfully</errorMsg>
      </errorMsg>
      <reportName>S-4_t4-2013-01-24-1611</reportName>
      <size>71680</size>
      <fazReportData>
      <reportContent>
      </fazReportData>
   </ns3:getFazGeneratedReportResponse>
</SOAP-ENV:Body>
```

Request Field	Description
<errorMsg>	Indicates if the request was successful or if it failed. The error message consists of the error code and detail.
<errorCode>	Error code and message details: • -101: Invalid username, password, or ADOM. Cannot get report name. Cannot get report date. • -104: Cannot find report name. Cannot find file in directory. Cannot read file in directory. • -106: Not enough memory.
<errorMsg>	
<reportName>	The generated report name. For example, S-schedule-utm-reports_t1-2013-01-24-1022.
<size>	The generated report size.
<fazReportData>	Report content data will be displayed under this element.

Request Field	Description
<reportContent>	Contains the actual report data. The data is base64 encoded, you need to decode the data before use.

getSystemStatus

Use this request to get system status information in the current system.

Example request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:getSystemStatus>
         <!--Optional:-->
         <servicePass>
            <!--Optional:-->
            <userID>admin</userID>
            <!--Optional:-->
            <password></password>
         </servicePass>
         <!--Optional:-->
         <adom>root</adom>
   </r20:getSystemStatus>
</soapenv:Body>
```

Request Field	Description
<servicePass>	XML structure consists of username and password variables.
<userID>	The administrator user name.
<password>	Administrator password options: • Enter the administrator password. • Leave field blank for no password.
<adom>	If the ADOM field is blank, it is assigned as root.

The response indicates if the request was successful or if it failed.

Example response:

```
<SOAP-ENV:Header/>
<SOAP-ENV:Body>
   <ns3:getSystemStatusResponse>
         <errorMsg>
         <errorCode>0</errorCode>
            <errorMsg>getSystemStatus successfully</errorMsg>
            </errorMsg>
         <platformType>FMG-VM64</platformType>
         <version>v5.0-build0114 130118 (Interim)</version>
         <serialNumber>FMG-VM0A11000137</serialNumber>
```

```
            <biosVersion>04000002</biosVersion>
            <hostName>FMG-VM64</hostName>
            <maxNumAdminDomains>1000000000</maxNumAdminDomains>
            <maxNumDeviceGroup>1000000000</maxNumDeviceGroup>
            <adminDomainConf>Enabled</adminDomainConf>
            <fipsMode>Disabled</fipsMode>
      </ns3:getSystemStatusResponse>
   </SOAP-ENV:Body>
```

Response Field	Description
<errorMsg>	Indicates if the request was successful or if it failed. The error message consists of the error code and detail.
<errorCode>	Error code and message details: • -101: Invalid username, password, or ADOM.
<errorMsg>	
<platformType>	Device model information.
<version>	The firmware version, v5.0-build0114 130118 (interim) for example.
<serialNumber>	The serial number of the device, FMG-VM0A11000137, for example.
<biosVersion>	The BIOS version of the device.
<hostName>	The device host name.
<maxNumAdminDomains>	The maximum number of ADOMs.
<maxNumDeviceGroup>	The maximum number of device groups.
<adminDomainConf>	ADOM mode status.
<fipsMode>	FIPS mode status.

getTaskList

Use this request to get a list of tasks as defined on your unit. Only an administrator with the `Super_User` profile can run this command.

Example request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:getTaskList>
         <servicePass>
            <password></password>
            <userID>admin</userID>
         </servicePass>
         <adom></adom>
         <taskId>1</taskId>
```

```
    </r20:getTaskList>
</soapenv:Body>
```

Request Field	Description
<servicePass>	XML structure consists of username and password variables.
<userID>	The administrator user name.
<password>	Administrator password options: • Enter the administrator password. • Leave field blank for no password.
<adom>	If the ADOM field is blank, the default ADOM will be that of the administrative user. If this administrator binds to all ADOMs, then the ADOM is root.
<taskId>	Indicates the task ID number. If the `<waitTask>` was false, then the task ID is displayed.

The response is a series of `<return>` tags, each containing information about a task.

Example response:

```
<SOAP-ENV:Header/>
<SOAP-ENV:Body>
   <ns3:getTaskListResponse>
         <errorMsg>
            <errorCode>0</errorCode>
            <errorMsg>Get task ID detail successfully</errorMsg>
         </errorMsg>
         <taskList>
            <taskId>1</taskId
            <source>5</source>
            <description>system checkpoint task</description>
            <userID>admin</userID>
            <status>4</status>
            <startTime>2012-09-29T15:18:22Z</startTime
         <deviceList>
            <devName>create system checkpoint</devName>
            <ip>0.0.0.0</ip>
            <status>4</status>
         <message>Create system checkpoint succeed</message>
         <history>
            <name>create system checkpoint</name>
            <percentage>0</percentage>
            <description>task start ...</description>
         </history>
         <history>
            <name>create system checkpoint</name>
            <percentage>5</percentage>
            <description>Lock system succeed</description>
         </history>
         ...
         ...
```

```
            </deviceList>
          </taskList>
    </ns3:getTaskListResponse>
</SOAP-ENV:Body>
```

Response Field	Description
<errorMsg>	Indicates if the request was successful or if it failed. The error message consists of the error code and detail.
<errorCode>	Error code and message details: • 0: Retrieved task ID detail successfully. • -101: Invalid task ID. The task ID is empty or invalid. • -102: The task ID does not exist. • -106: Not enough memory.
<errorMsg>	
<taskList>	XML structure consists of the task ID, source, description, user ID, status, and start time variables.
<taskId>	Indicates the task ID number. If the `<waitTask>` was false, then the task ID is displayed.
<source>	Indicates the source of the task: • 0: Device manager • 1: Security console • 2: Copy global object • 3: Install configuration • 4: Script execution • 5: System checkpoint • 6: Import device policy • 7: Install EMS global policy
<description>	Describes the list.
<userID>	The administrator user name.
<status>	Indicates the status of the task: • 1: running • 2: cancelling • 3: cancelled • 4: done • 5: error • 6: aborting • 7: aborted
<startTime>	Indicates the time the task list started.
<deviceList>	XML structure consists of the device name, IP, status, and description.

Response Field	Description
<devName>	Name of the device host.
<ip>	The device IP address.
<status>	Status of the device.
<message>	Description of the task.
<history>	
<name>	The history name.
<percentage>	Percentage of progress bar of each task that has been applied to the device.
<description>	Description of the history.

listFazGeneratedReports

Use this request to list FortiAnalyzer generated reports.

Example request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:listFazGeneratedReports>
      <!--Optional:-->
      <servicePass>
         <!--Optional:-->
         <userID>admin</userID>
         <!--Optional:-->
         <password></password>
      </servicePass>
      <!--Optional:-->
      <adom>root</adom>
      <!--Optional:-->
      <startDate>2013-02-04T00:00:00</startDate>
      <!--Optional:-->
      <endDate>2013-02-05T00:00:00</endDate>
   </r20:listFazGeneratedReports>
</soapenv:Body>
```

Request Field	Description
<servicePass>	XML structure consists of username and password variables.
<userID>	The administrator user name.

Request Field	Description
<password>	Administrator password options: Enter the administrator password or leave field blank for no password.
<adom>	The ADOMs for which you want to list a generated reports.
<startDate>	The report start date.
<endDate>	The report end date.

The response indicates if the request was successful or if it failed.

Example response:

```
<SOAP-ENV:Header/>
<SOAP-ENV:Body>
   <ns3:listFazGeneratedReportsResponse>
      <errorMsg>
         <errorCode>0</errorCode>
         <errorMsg>listFazGeneratedReports successfully</errorMsg>
      </errorMsg>
      <totalNumberExists>48</totalNumberExists>
      <reportList>
         <reportName>S-schedule-utm-reports_t1-2013-02-04-0000</reportName>
         <startTime>2013-02-04T08:00:03Z</startTime>
         <endTime>2013-02-04T08:02:44Z</endTime>
         <reportProgressPercent>100</reportProgressPercent>
         <size>52122</size>
         <formats>PH</formats>
      </reportList>
   </ns3:listFazGeneratedReportsResponse>
</SOAP-ENV:Body>
```

Request Field	Description
<errorMsg>	Indicates if the request was successful or if it failed. The error message consists of the error code and detail.
<errorCode>	Error code and message details: • -101: Invalid username, password, or ADOM. No reports are available. • -104: Cannot get report counts. • -106: Not enough memory.
<errorMsg>	
<totalNumberExists>	All available reports in FortiAnalyzer.
<reportList>	XML structure consists of report name, start time, end time, report progress, size, and format variables.

Request Field	Description
<reportName>	The generated report name. For example, `S-schedule-utm-reports_t1-2013-01-24-1022`.
<startTime>	Indicates the time the report started.
<endTime>	Indicates the time the report ended.
<reportProgressPercent>	Report running progress; 0 to 100%.
<size>	The generated report size.
<formats>	The report format: • P: PDF • H: HTML • T: TXT

removeFazArchive

Use this command to remove a FortiAnalyzer archive.

Example request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:removeFazArchive>
      <!--Optional:-->
      <servicePass>
         <!--Optional:-->
         <userID>admin</userID>
         <!--Optional:-->
         <password></password>
      </servicePass>
      <!--Optional:-->
      <adom>root</adom>
      <!--Optional:-->
      <devId>FG200B0000000001</devId>
      <!--Optional:-->
      <type>IPS</type>
      <!--Optional:-->
      <fileName>50008:0</fileName>
      <!--Optional:-->
      <checksum>?</checksum>
   </r20:removeFazArchive>
</soapenv:Body>
```

Request Field	Description
<servicePass>	XML structure consists of username and password variables.

Request Field	Description
<userID>	The administrator user name.
<password>	Administrator password options: Enter the administrator password or leave field blank for no password.
<adom>	The ADOM for which you want to remove the FortiAnalyzer archive.
<devId>	The device ID. This is the primary device identifier.
<type>	The archive type. Archive type options: • 0: Web • 1: Email • 2: FTP • 3: IM • 4: MMS • 5: Quarantine • 6: IPS
<fileName>	Shows the name of the file. Note: the file name cannot start with a | or a ~ character.
<checksum>	Checksum is used when the type is Quarantine. Checksum is used instead of filename.

The response indicates if the request was successful or if it failed.

Example response:

```
<SOAP-ENV:Header/>
<SOAP-ENV:Body>
   <ns3:removeFazArchiveResponse>
      <errorMsg>
         <errorCode>0</errorCode>
         <errorMsg>removeFazArchive successfully</errorMsg>
      </errorMsg>
   </ns3:removeFazArchiveResponse>
</SOAP-ENV:Body>
```

Request Field	Description
<errorMsg>	Indicates if the request was successful or if it failed. The error message consists of the error code and detail.
<errorCode>	Error code and message details: • -101: Invalid username, password, or ADOM. Cannot get the device ID. Cannot get the file name. Cannot get the type. Cannot get the checksum. • -104: Cannot delete content archive file.
<errorMsg>	

runFazReport

Use this request to run a report through web services. You need to input the schedule name of the report. In v5.2 Patch Release 2 or later you can add filters to support per user reports. `runFazReport` supports up to 10k filters.

Example request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:runFazReport>
      <!--Optional:-->
      <servicePass>
         <!--Optional:-->
         <userID>admin</userID>
         <!--Optional:-->
         <password></password>
      </servicePass>
      <!--Optional:-->
      <adom>root</adom>
      <!--Optional:-->
      <reportTemplate>12</reportTemplate>
      <filter>user=USER00001</filter>
      <filter>user=USER00002</filter>
   </r20:runFazReport>
</soapenv:Body>
```

Request Field	Description
<servicePass>	XML structure consists of username and password variables.
<userID>	The administrator user name.
<password>	Administrator password options: Enter the administrator password or leave field blank for no password.
<adom>	The ADOMs for which you want to run a report against.
<reportTemplate>	The name of the report template.
<filter>	Add filters to create per-user reports.

The response indicates if the request was successful or if it failed.

Example response:

```
<SOAP-ENV:Header/>
<SOAP-ENV:Body>
   <ns3:runFazReportResponse>
      <errorMsg>
         <errorCode>0</errorCode>
         <errorMsg>runFazReport successfully</errorMsg>
      </errorMsg>
```

```
      <reportTemplate>12</reportTemplate>
   </ns3:runFazReportResponse>
</SOAP-ENV:Body>
```

Request Field	Description
<errorMsg>	Indicates if the request was successful or if it failed. The error message consists of the error code and detail.
<errorCode>	Error code and message details: • -101: Invalid username, password, or ADOM. Cannot get report schedule name. • -104: Cannot get report schedule name from SQL.
<errorMsg>	
<reportTemplate>	The name of the report template.

searchFazLog

Use this request to provide raw logs in FortiAnalyzer per conditions set in the request. You need to input the log format, device name, log type, search criteria, start index, and maximum return value in the request message body.

Example request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:searchFazLog>
      <!--Optional:-->
      <servicePass>
         <!--Optional:-->
         <userID>admin</userID>
         <!--Optional:-->
         <password></password>
      </servicePass>
      <!--Optional:-->
      <adom>root</adom>
      <!--Optional:-->
      <content>logs</content>
      <!--Optional:-->
      <format>rawFormat</format>
      <!--Optional:-->
      <deviceName>FG200B-1</deviceName>
      <logType>traffic</logType>
      <!--Optional:-->
      <searchCriteria>srcip=10.0.0.1</searchCriteria>
      <maxNumMatches>30</maxNumMatches>
      <startIndex>1</startIndex>
      <checkArchive>0</checkArchive>
      <!--Optional:-->
      <DLPArchiveType>1</DLPArchiveType>
      <!--Optional:-->
      <compression>tar</compression>
   </r20:searchFazLog>
```

```
</soapenv:Body>
```

Request Field	Description
<servicePass>	XML structure consists of username and password variables.
<userID>	The administrator user name.
<password>	Administrator password options: Enter the administrator password or leave field blank for no password.
<adom>	The ADOMs for which you want to search logs.
<content>	The log contents you want to search. Log content options: • 0: Logs • 1: Content logs • 2: Local logs
<format>	The log formats to display. Log format options: • 0: Raw • 1: CSV
<deviceName>	The device name you want to search logs from.
<logType>	Type of logs you want to search. Log type options: • 0: Event • 1: Traffic • 2: Attack • 3: Antivirus • 4: Web logs • 5: IM • 6: Email • 7: Content • 8: History • 9: Generic • 10: VoIP • 11: DLP • 12: Application Control • 13: Network Scanning
<searchCriteria>	The search criteria used to search logs. For example, vd-root.
<maxNumMatches>	The maximum number of matches to display from the search results.
<startIndex>	The start index of the matched logs.
<checkArchive>	This variable is not used. Always set the value to 0.

Request Field	Description
<DLPArchiveType>	The DLP archive type. DLP archive type options: • 0: Web • 1: Email • 2: FTP • 3: IM • 4: MMS • 5: Quarantine • 6: IPS
<compression>	The compression type of the report that will be returned by this command. Compression options: • 0: tar • 1: gzip

The response will contain the logs that match the criteria specified in the request.

Example response:

```
<SOAP-ENV:Header/>
<SOAP-ENV:Body>
   <ns3:searchFazLogResponse>
      <errorMsg>
         <errorCode>0</errorCode>
         <errorMsg>searchFazLog successfully</errorMsg>
      </errorMsg>
      <totalResultsFound>300</totalResultsFound>
      <matchesReturned>16</matchesReturned>
      <startIndex>1</startIndex>
      <logs>
         <data>
            <logEntry>date=2013-01-25 time=09:50:58 itime=1359107458 logid=2222222222
                type=ips subtype=status=accept level=level40 devid=FG200B0000000001
                policyid=10000 sessionid=10000 attackid=10000 severity=severity
                profile=profile40 sensor=sensor40 srcip=10.0.0.1 dstip=10.0.0.1
                srcport=1000 icmpid=icmpid40 dstport=1000 icmptype=icmpty icmpcode=icmpco
                srcintf=srcintf40 dstintf=dstintf40 proto=0 service=smtp user=user1
                group=group40 ref=ref40 count=10000 incidentserialno=10000 msg=msg40 vd=vd1
                identidx=10000 profiletype=profiletype40 profilegroup=prof
                attackname=attackname40 direction=10000 dstname=dstname40 srcname=srcname40
                agent=agent40 osname=osname40 osversion=osversion40 unauthuser=unauthuser40
                unauthusersource=unauthusersource40 eventtype=eventtype40</logEntry>
         </data>
      </logs>
   </ns3:searchFazLogResponse>
</SOAP-ENV:Body>
```

Request Field	Description
<errorMsg>	Indicates if the request was successful or if it failed. The error message consists of the error code and detail.

Request Field	Description
<errorCode>	Error code and message details: • -101: Invalid username, password, or ADOM. Cannot get device name. Cannot get search criteria. Incorrect DLP archive type. • -102: Cannot find device name on system. • -104: Cannot find logs with criteria. • -106: Not enough memory.
<errorMsg>	
<totalResultsFound>	The total number of logs found.
<matchesReturned>	The total number of logs which matched the search criteria.
<startIndex>	The start index in the request.
<logs>	Log data will be displayed under this element.
<logEntry>	Displays log data.

setFazConfig

Use this request to set the FortiAnalyzer configuration. You can set either partial or full configuration.

Example request:

```
<soapenv:Header/>
<soapenv:Body>
   <r20:setFazConfig>
      <!--Optional:-->
      <servicePass>
         <!--Optional:-->
         <userID>admin</userID>
         <!--Optional:-->
         <password></password>
      </servicePass>
      <!--Optional:-->
      <adom>root</adom>
      <!--Optional:-->
      <config>
   config system global
      set adom-mode normal
      set hostname "FMG-VM"
   end
   config system interface
      edit "port1"
         set ip 172.16.106.254 255.255.255.0
         set allowaccess ping https ssh http webservice
         set serviceaccess fgtupdates webfilter-antispam webfilter antispam
            config ipv6
            end
      next
```

```
   edit "port2"
      set ip 1.2.2.2 255.255.255.0
      set allowaccess ping https ssh http webservice
      set serviceaccess fgtupdates webfilter-antispam webfilter antispam
         config ipv6
         end
   next
   edit "port3"
         config ipv6
         end
   next
   edit "port4"
         config ipv6
         end
   next
end
config system snmp sysinfo
end
config system route
   edit 1
      set device "port1"
      set gateway 172.16.106.1
   next
end
config system dns
   set primary 208.91.112.53
   set secondary 208.91.112.63
end
config system ha
end
config system ntp
config ntpserver
   edit 1
      set server "ntp1.fortinet.net"
   next
   end
      set status enable
      set sync_interval 1
end
config system backup all-settings
end
config system metadata admins
   edit "Contact Email"
      set importance optional
   next
   edit "Contact Phone"
      set importance optional
   next
end
config system admin profile
   edit "Restricted_User"
      set description "Restricted user profiles have no System Privileges enabled, and
          have read-only access for all Device Privileges."
      set device-manager read
      set device-config read
      set device-profile read
      set policy-objects read
```

```
            set deploy-management read
            set config-retrieve read
            set term-access read
            set adom-policy-packages read
            set adom-policy-objects read
            set vpn-manager read
            set realtime-monitor read
            set forticonsole read
            set consistency-check read
            set faz-management read
            set log-viewer read
            set report-viewer read
        next
        edit "Standard_User"
            set description "Standard user profiles have no System Privileges enabled, but
                have read/write access for all Device Privileges."
            set adom-switch read-write
            set global-policy-packages read-write
            set global-objects read-write
            set device-manager read-write
            set device-config read-write
            set device-op read-write
            set device-profile read-write
            set policy-objects read-write
            set deploy-management read-write
            set config-retrieve read-write
            set term-access read-write
            set adom-policy-packages read-write
            set adom-policy-objects read-write
            set vpn-manager read-write
            set realtime-monitor read-write
            set forticonsole read-write
            set consistency-check read-write
            set faz-management read-write
            set log-viewer read-write
            set report-viewer read-write
        next
        edit "Super_User"
            set description "Super user profiles have all system and device privileges
                enabled."
            set system-setting read-write
            set adom-switch read-write
            set global-policy-packages read-write
            set global-objects read-write
            set assignment read-write
            set read-passwd read-write
            set device-manager read-write
            set device-config read-write
            set device-op read-write
            set device-profile read-write
            set policy-objects read-write
            set deploy-management read-write
            set config-retrieve read-write
            set term-access read-write
            set adom-policy-packages read-write
            set adom-policy-objects read-write
            set vpn-manager read-write
```

```
            set realtime-monitor read-write
            set forticonsole read-write
            set consistency-check read-write
            set faz-management read-write
            set log-viewer read-write
            set report-viewer read-write
        next
        edit "Package_User"
            set description "Package user profile have read/write policy package and objects
                privileges enabled, and have read-only access for system and others
                privileges."
            set system-setting read
            set adom-switch read
            set global-policy-packages read-write
            set global-objects read-write
            set assignment read
            set read-passwd read
            set device-manager read-write
            set device-config read-write
            set device-op read-write
            set device-profile read-write
            set policy-objects read-write
            set deploy-management read-write
            set config-retrieve read
            set term-access read
            set adom-policy-packages read-write
            set adom-policy-objects read-write
            set vpn-manager read-write
            set realtime-monitor read
            set forticonsole read
            set consistency-check read
            set faz-management read
            set log-viewer read
            set report-viewer read
        next
    end
    config system certificate ca
    end
    config system certificate local
    end
    config system password-policy
    end
    config system admin user
        edit "admin"
            set trusthost2 0.0.0.0 0.0.0.0
            set trusthost3 127.0.0.1 255.255.255.255
            set ipv6_trusthost2 ::/0
            set ipv6_trusthost3 ::1/128
            set profileid "Super_User"
            set adom "all_adoms"
            set policy-package "all_policy_packages"
    config dashboard
        edit 1
            set name "System Information"
            set column 1
            set refresh-interval 0
            set tabid 1
```

```
      set widget-type sysinfo
      next
   edit 2
      set name "System Resources"
      set column 1
      set refresh-interval 0
      set tabid 1
      set widget-type sysres
      set res-view-type real-time
      next
   edit 3
      set name "License Information"
      set column 2
      set refresh-interval 0
      set tabid 1
      set widget-type licinfo
      next
   edit 4
      set name "Unit Operation"
      set column 2
      set refresh-interval 0
      set tabid 1
      set widget-type sysop
      next
   edit 5
      set name "Alert Message Console"
      set column 2
      set refresh-interval 0
      set tabid 1
      set widget-type alert
      set num-entries 0
      next
   end
   next
end
config system admin setting
end
config system alertemail
end
config system mail
   edit "mail.fortinet.com"
      set auth enable
      set passwd ENC
          26ITYiEXHPFvx8y3vZqI4PPt2dH0OXAWPB3sVNcK+2nPTGyeRN1FMB+hJIlyHsyzchBxBmA2EMZEj
          y4gR5vBnYiufPp2Q5rcGhSAYqGQ2zMSt79R
      set user "jsmith@fortinet.com"
      next
   end
config system alert-console
end
config system log fortianalyzer
end
config system locallog disk setting
end
config system locallog disk filter
end
config system locallog memory setting
```

```
end
config system locallog memory filter
end
config system locallog fortianalyzer setting
end
config system locallog fortianalyzer filter
end
config system locallog syslogd setting
end
config system locallog syslogd filter
end
config system locallog syslogd2 setting
end
config system locallog syslogd2 filter
end
config system locallog syslogd3 setting
end
config system locallog syslogd3 filter
end
config system fips
end
config fmupdate av-ips fgt server-override
end
config fmupdate av-ips fct server-override
end
config fmupdate web-spam fgt server-override
end
config fmupdate web-spam fct server-override
end
config fmupdate av-ips push-override
end
config fmupdate av-ips push-override-to-client
end
config fmupdate web-spam poll-frequency
end
config fmupdate av-ips web-proxy
end
config fmupdate web-spam web-proxy
end
config fmupdate fct-services
end
config fmupdate av-ips advanced-log
end
config fmupdate av-ips update-schedule
end
config fmupdate analyzer virusreport
end
config fmupdate service
end
config fmupdate publicnetwork
end
config fmupdate disk-quota
end
config fmupdate server-access-priorities
end
config fmupdate web-spam fgd-setting
end
```

```
      config fmupdate web-spam fgd-log
      end
      config fmupdate custom-url-list
      end
      config fmupdate device-version
      end
      config fmupdate deployment
      end
      config fmupdate server-override-status
      end
      config fmupdate multilayer
      end
      config fmupdate support-pre-fgt43
      end
      config system dm
      end
      config system log settings
      config rolling-regular
      end
      end
         config system sql
            set start-time 09:37 2013/01/18
         end
         </config>
      </r20:setFazConfig>
   </soapenv:Body>
```

Request Field	Description
<servicePass>	XML structure consists of username and password variables.
<userID>	The administrator user name.
<password>	Administrator password options: Enter the administrator password or leave field blank for no password.
<adom>	The ADOMs for which you want to set the configuration.
<config>	The configuration content to be sent.

The response indicates if the request was successful or if it failed.

Example response:

```
<SOAP-ENV:Header/>
<SOAP-ENV:Body>
   <ns3:setFazConfigResponse>
      <errorMsg>
         <errorCode>0</errorCode>
         <errorMsg>setFazConfig failed</errorMsg>
      </errorMsg>
      <cliError>command parse error before 'webfilter'
      (port1)#</cliError>
      <errorLineNumber>10</errorLineNumber>
   </ns3:setFazConfigResponse>
</SOAP-ENV:Body>
```

Request Field	Description
<errorMsg>	Indicates if the request was successful or if it failed. The error message consists of the error code and detail.
<errorCode>	Error code and message details: • -101: Invalid username, password, or ADOM. Cannot get configuration value. • -104: Cannot set configuration.
<errorMsg>	
<errorLineNumber>	The line number where the error occurs.